

**UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF VIRGINIA  
Alexandria Division**

SHARYL THOMPSON ATTKISSON,  
JAMES HOWARD ATTKISSON,  
SARAH JUDITH STARR ATTKISSON,

Plaintiffs,

v.

Civil Action No. 1:17-cv-1474

UNITED STATES OF AMERICA,

Defendant.

---

**PLAINTIFFS' COMPLAINT**

---

Plaintiffs, by and through undersigned counsel, submit the following Complaint:

1. This case is brought pursuant to the Federal Tort Claims Act ("FTCA"), 28 U.S.C. § 2671 et seq. and the law of the Commonwealth of Virginia. The matter is brought as a related case to the previously filed action brought against federal officials under docket number/Civil Action No. 1:17-cv-364-LMB.

**JURISDICTION AND VENUE**

2. The Court has jurisdiction over the subject matter of this Complaint under 28 U.S.C. §§ 1331 & 1346(b).

3. On December 26, 2014, Plaintiffs submitted an Administrative Tort Claim to the United States Department of Justice and the United States Postal Service as required by law. Plaintiffs' claim was deemed denied pursuant to 28 U.S.C. § 2675(a) by virtue of Claimants/Plaintiffs receiving no response from the respective federal agencies within six

months of filing. Plaintiffs have therefore exhausted all available administrative remedies, and satisfied all conditions precedent, to the filing of suit.

4. Plaintiffs filed suit against the United States and others on September 2, 2015 in the United States District Court for the District of Columbia, Civil Action No. 1:15-cv-01437-EGS. Following transfer to the Eastern District of Virginia, the United States was dismissed as a party without an adjudication on the merits of the claim against them on September 15, 2017. Pursuant to 28 U.S.C. §2401 and Va. Code 8.01-229(E)(1), this case is therefore timely (re)filed.

5. Venue is proper under 28 U.S.C. § 1402(b) in that a substantial part of the conduct that forms the basis for the allegations occurred within the District.

### **PARTIES**

6. At all times relevant to the subject lawsuit, Plaintiff Sharyl Attkisson was a citizen and resident of Leesburg, Virginia, and an investigative reporter for CBS News. Plaintiff was responsible for investigating, writing, publishing, and airing investigative news stories on a wide-variety of topics, including the federal gun-trafficking investigation that came to be known as "*Fast and Furious*," and the controversial attack of the American diplomatic mission in Benghazi, Libya.

7. At all times relevant to the subject lawsuit, Plaintiff James Howard Attkisson was a citizen and resident of Leesburg, Virginia, and was married to Sharyl Attkisson. Because much of the surveillance alleged in this complaint occurred at their shared residence, Mr. Attkisson was subjected to surveillance as well, and his confidential, professional, and personal information was illegally accessed.

8. At all times relevant to the subject lawsuit, Plaintiff Sarah Judith Starr Attkisson was a citizen and resident of Leesburg, Virginia, and the daughter of James and Sharyl

Attkisson. Because much of the surveillance alleged in this complaint occurred at Sarah Attkisson's residence, she was subjected to surveillance as well, and her confidential, professional, and personal information were illegally accessed.

9. The United States of America is the proper party defendant pursuant to the Federal Tort Claims Act in that all of the actions described herein were taken by persons believed to be acting on behalf of the United States, either as employees of the United States or independent contractors hired by an agency of the United States.

### **BACKGROUND**

10. During all times relevant to the subject Complaint, Sharyl Attkisson was an investigative reporter for CBS News. She served CBS for twenty (20) years. Her job required her to investigate and report on national news stories. In 2011, during the course of her reporting, Plaintiff began investigating what later became known as the "*Fast and Furious*" gun-walking story involving federal agents from the Bureau of Alcohol, Tobacco, and Firearms (ATF) improperly permitting weapons to pass into the hands of the Mexican drug cartels.

11. Her first *Fast and Furious* report aired on CBS on February 22, 2011. The report quoted and relied upon numerous confidential sources, all of whom were critical of the *Fast and Furious* gun-walking strategy deployed by the respective federal agencies.

12. In February, 2011, the ATF, in an internal memorandum, instigated an orchestrated campaign against Ms. Attkisson's report, including efforts to discredit it, and outlined a strategy for the Agency to push "positive stories" in order to "preempt some negative reporting."<sup>1</sup>

---

<sup>1</sup> See [http://www.cbsnews.com/8301-31727\\_162-20039251-10391695.html](http://www.cbsnews.com/8301-31727_162-20039251-10391695.html)

13. Despite the foregoing efforts, Ms. Attkisson continued to report *Fast and Furious* stories. When contacted for comment, DOJ officials persisted in their denial of the allegations and continued efforts to unveil Ms. Attkisson's confidential sources. ATF sources told Ms. Attkisson that the Agency was actively seeking to identify government insiders who were providing information or "leaking" to her and CBS.

14. In September 2011, Ms. Attkisson reported on secret audio recordings that implicated the FBI in an alleged discrepancy in its accounting of evidence in the *Fast and Furious* related murder of Border Patrol Agent Brian Terry.

15. Also in September 2011, Ms. Attkisson reported on the alleged involvement of an F.B.I. informant in the *Fast and Furious* matter.

16. In October 2011, Ms. Attkisson reported on the continuing controversy regarding the F.B.I.'s accounting of evidence in *Fast and Furious*.

17. In November 2011, Ms. Attkisson reported on evidence contradicting then-Attorney General Eric Holder's sworn testimony wherein he claimed that he had only heard of *Fast and Furious* for the first time in the past couple of weeks.

18. In December 2011, Ms. Attkisson reported on the DOJ's formal retraction of a letter and a misrepresentation made to Congress in February 2011, which had stated, incorrectly, that there had been no "gun-walking."

19. In mid-to-late 2011, Ms. Attkisson, Mr. Attkisson, and Sarah Attkisson began to notice anomalies in numerous electronic devices at their home in Virginia. These anomalies included a work Toshiba laptop computer and a family Apple desktop computer turning on and off at night without input from anyone in the household, the house alarm chirping daily at different times, often indicating "phone line trouble," and television problems, including

interference. All of the referenced devices use the Verizon FiOS line installed in Plaintiffs' home. Verizon was unable to cure the problems, despite multiple attempts over a period of more than a year.

20. In January 2012, Ms. Attkisson contacted Verizon about ongoing internet problems and intermittent connectivity because the residential internet service began constantly dropping off. She had not experienced similar problems previously. In response to the complaint, Verizon sent a new router, which was immediately installed. The new router failed to resolve the issues.

21. In February 2012, an unauthorized party or parties remotely installed sophisticated surveillance spyware on Ms. Attkisson's Toshiba laptop. The invasion was unknown to Ms. Attkisson at the time, but revealed later by forensic computer analysis, including factual evidence demonstrating that Plaintiffs' computer systems were targets of unauthorized surveillance efforts, including prolonged ongoing surveillance of the iMac. From artifacts remaining on the iMac, the intrusions were occurring as early as June, 2011.

22. The forensic analysis likewise revealed direct targeting of Plaintiffs' Blackberry mobile phone when connected to the iMac. Records reveal a file recovery process performed by an intruder that transferred large numbers of records off the BlackBerry. Changes to VPN settings were likewise found as the enabling of the built in Ethernet connection, after years of not being used, reflect further clear evidence of unauthorized surveillance activities. The issuing of the *smbclient* command along with recovered records showing the iMac mounted as a network shared resource, is further evidence of uninvited, remote surveillance designed to enable the contents on the iMac to be easily exposed as well as exfiltrated.

23. From available forensic evidence, the unauthorized intruder maintained complete control of Plaintiffs system during the referenced time-frame. Access to e-mails, personal files, Internet browsing, passwords, execution of programs, financial records, photographs of not just the Plaintiffs, but of their family members, was likewise achieved. With regard to attribution, information recovered directly from Plaintiffs' computer during forensic analysis proved that remote communication with Plaintiffs' system was executed via IP addresses owned, controlled, and operated by the United States Postal Service, and was not associated with any web server or website used by the USPS. Attempts to communicate with the IP addresses were rejected. Specifically, Internet Protocol version 6 ("IPv6") address 385b:8f09:80fa:ffff:385b:8f09:80fa:ffff belonging to the USPS was discovered on Plaintiff's laptop, and this IPv6 address was used as part of a "zero-day" attack against Plaintiff, along with the two previously disclosed USPS IPv4 addresses. According to the US Government's Committee on National Security Systems ("CNSS"), a zero-day attack "exploits a previously unknown hardware, firmware, or software vulnerability".<sup>2</sup> Here, the previously unknown software vulnerability used to exploit Plaintiff's laptop remotely—using at least three USPS IP addresses—involved Intel Corporation's Active Management Technology ("AMT") software.<sup>3</sup> As detailed below, only the FBI has the necessary legal authorities and resources to conduct an APT-style cyber-attack in the United States against Plaintiff, a US Person ("USP") and member of the news media, using a zero-day vulnerability in combination with multiple IP addresses owned by the USPS.

---

<sup>2</sup> See *Committee on National Security Systems (CNSS) Glossary*, Apr 5, 2015, online at <https://csrc.nist.gov/Glossary/?term=2541>.

<sup>3</sup> See *About the Intel Manageability Firmware Critical Vulnerability*, May 26, 2017, online at <https://www.intel.com/content/www/us/en/architecture-and-technology/intel-amt-vulnerability-announcement.html>

24. During the relevant time period, Verizon was providing bulk metadata to the FBI, including metadata from Plaintiff Sharyl Attkisson's CBS mobile phone, personal home phone, and personal home Internet connection by way of an FISA court order. Forensic evidence shows that Verizon employees and/or personnel were involved in the tapping of Plaintiff Attkisson's fiber-optic telecommunication line (supporting "downstream" collection for the US Government). A Verizon mobile WiFi hot-spot was also used to connect to Plaintiff Attkisson's CBS laptop for surveillance and data exfiltration by the US Government (Verizon MiFi 4510L). It is likely that a Verizon Inmarsat BGAN mobile satellite terminal was used to connect to Plaintiff Attkisson's CBS laptop for surveillance and data exfiltration by the US Government. Likewise, Verizon used USPS-owned IP addresses to support the US Government's surveillance and data exfiltration against Plaintiff Attkisson.

25. Having no idea that the Government and Verizon were cooperating, in February 2012, Ms. Attkisson contacted Verizon yet again to complain about continuing anomalies.

26. In March 2012, a Verizon representative visited Ms. Attkisson's home and replaced the router a second time. The representative also replaced the entire outside FiOS service box. Despite Verizon's efforts, however, the anomalies persisted.

27. In April-May, 2012, the DOJ and FBI publicly announced a new effort to vastly expand cyber related efforts to address alleged "national security-related cyber issues." During the same time frame, the DOJ secretly--and without notice--seized personal and phone records belonging to journalists from the Associated Press news agency in violation

longstanding DOJ practice. The records seizure was not publicly known at the time, but was later revealed.<sup>4</sup>

28. In July 2012, the DOJ designated U.S. Attorneys' offices to act as "force multipliers" in its stepped-up cyber efforts in the name of national security.<sup>5</sup>

29. That same month, July 2012, intruders remotely "refreshed" the ongoing surveillance of Ms. Attkisson's Toshiba computer. Again, the access was unknown to Ms. Attkisson at the time, but was revealed later through computer forensic analysis.

30. In September, 2012, Wikileaks published internal emails from a global intelligence company doing business with government agencies. The materials made reference to "Obama leak investigations" and the alleged "witch hunts of investigative journalists learning information from inside the beltway sources." The email states, "(T)here is a specific tasker from the [White House] to go after anyone printing materials negative to the Obama agenda (oh my.) Even the FBI is shocked."

31. On October 5, 2012, CBS aired Ms. Attkisson's first Benghazi story for CBS, which was critical of the Executive Branch's handling of the security requests at the U.S. compound in Benghazi, Libya, where Ambassador Christopher Stevens and three (3) other U.S. personnel were killed on September 11, 2012.

32. On October 8, 2012, CBS aired another Attkisson report on Benghazi that included an interview with whistleblower Col. Andrew Wood. During the weeks following the airing of Col. Wood's interview, Ms. Attkisson made personal contact with numerous confidential sources within the federal government (or who had links to intelligence

---

<sup>4</sup> <http://blogs.justice.gov/main/archives/date/2012/11>

<sup>5</sup> [http://www.wikileaks.org/gifiles/docs/1210665\\_obama-leak-investigations-internal-use-only-pls-do-not.html](http://www.wikileaks.org/gifiles/docs/1210665_obama-leak-investigations-internal-use-only-pls-do-not.html) (last accessed on October 28, 2014).

agencies within the U.S. government). The confidential government sources reported to Ms. Attkisson that efforts were being made by the Executive Branch to clamp down on leaks and to track the leaking of information to specific reporters regarding the Benghazi affair.

33. In the later part of October 2012, Ms. Attkisson, Mr. Attkisson, and Sarah Attkisson began noticing an escalation of electronic problems at their personal residence, including interference in home and mobile phone lines, computer interference, and television interference. They were still unaware of any intrusion, however.

34. During the same general time frame, several sources with close ties to the intelligence community approached Ms. Attkisson privately and informed her that the government would likely be monitoring her electronically in an effort to identify her confidential sources, and also to monitor her continued *Fast and Furious* and *Benghazi* stories.

35. In November 2012, Ms. Attkisson's phone line became nearly unusable because of anomalies and interruptions. Her mobile phones also experienced regular interruptions and interference, making telephone communications unreliable, and, at times, virtually impossible.

36. In December 2012, Ms. Attkisson discussed her phone and computer issues with friends, contacts, and sources, via her home phone, mobile phones, and email. She decided to begin logging the times and dates that the computers turned on at night without her input. Soon after these phone and email discussions, the computer nighttime activity stopped.

37. Computer forensic analysis later revealed that the intruders executed remote actions in December 2012, to remove evidence of the intrusion from Ms. Attkisson's computers and home electronic equipment.

38. In December 2012, a contact with U.S. government intelligence experience conducted an inspection of Ms. Attkisson's exterior home. During the course of the inspection, the consultant discovered an anomaly with Ms. Attkisson's FiOS (Verizon) box: an extra fiber optics line was dangling from the exterior of the box.

39. Based on the odd finding, Ms. Attkisson contacted Verizon on December 31, 2012, which denied it had installed or had knowledge of the extraneous fiber optics line affixed to the equipment at the Attkisson's home and suggested Attkisson contact law enforcement authorities. Shortly thereafter, a person identifying herself as a Verizon supervisor telephoned Ms. Attkisson to advise her she was dispatching a technician to the house. It would be New Year's Day, so Ms. Attkisson informed the purported supervisor that it was unnecessary to dispatch a technician just then, and she offered to send them a photograph of the stray fiber optics line to save Verizon the trip. The purported supervisor declined the photograph and insisted that a technician would be present on New Year's Day.

40. On January 1, 2013, a person represented to be a Verizon technician visited the Attkisson's home and removed the additional fiber optics cable from the system. Ms. Attkisson asked the technician to leave the cable. The technician placed it next to the equipment and left the home. When Ms. Attkisson's husband arrived home and went to retrieve the extraneous cable, the cable had already been removed and was no longer on the premises.

41. Throughout the month of January 2012, Ms. Attkisson repeatedly contacted the purported Verizon technician to seek the location of the missing cable. The person representing himself as a technician never returned any of the calls at the number he had provided.

42. In January and February of 2013, Plaintiffs continued to experience phone and internet usage issues, including drop-offs, noises, and other interference. Verizon was notified and technicians and supervisors made additional contacts and visits.

43. On January 8, 2013, Ms. Attkisson made arrangements to deliver her Toshiba laptop to an individual with special expertise in computer forensics. On January 9, 2013, the forensics expert reported to Ms. Attkisson that the Toshiba laptop showed clear evidence of outside and unauthorized "intrusion," and that the sources of the intrusion were state-supported due to the sophisticated nature of the technology used.

44. On January 10, 2013, the computer was returned to Ms. Attkisson, along with a report. According to the report, the forensics computer expert found that sophisticated software had been used to accomplish the intrusion, and the software fingerprint indicated the software was proprietary to the federal government. The intrusion included, among other surveillance, keystroke monitoring, exfiltration of data, audio surveillance of Plaintiffs' conversations and activities at home by activating Skype, mining personal passwords, monitoring work and personal email, and probable compromise of Plaintiffs' work and personal smartphones.

45. According to the report, the surveillance by the identified software spanned most of 2012 at least. The report also stated the intruders had accessed CBS network systems, such as the ENPS program, and that the perpetrator had also placed three classified documents deep in the computer's operating system. Ms. Attkisson thereafter notified her direct supervisor at CBS News of the laptop intrusion and findings.

46. On February 2, 2013, an independent forensic computer analyst retained by CBS News spent approximately six (6) hours at Ms. Attkisson's home, during which time

he reported finding evidence on both Ms. Attkisson's Toshiba laptop and Apple desktop computers of a coordinated, highly-skilled series of actions and attacks directed at the operation of the computers and the storage and access of data thereon. CBS engaged the company to do further analysis of the Toshiba laptop in an attempt to recover wiped data.

47. In March 2013, Ms. Attkisson's Apple desktop computer began malfunctioning and, after several days of it freezing and emitting a burning odor, it shut down. Ms. Attkisson was unable to turn the Apple computer back on after this event.

48. On April 3, 2013, Ms. Attkisson filed a complaint with the DOJ Inspector General.

49. On May 6, 2013, an official with the United States Inspector General's office called Ms. Attkisson and stated that he had checked with the FBI, and the FBI denied any knowledge of any operations concerning Ms. Attkisson's computers or phone lines. The official also stated that there was no PATRIOT Act related order authorizing surveillance of Ms. Attkisson.

50. On May 21, 2013, Ms. Attkisson publicly stated in a radio interview her belief that her computers had been compromised, but did not assign or allege responsibility. A news outlet sought a statement from the DOJ regarding Ms. Attkisson's assertions. The DOJ issued a written response stating, "To our knowledge, the Justice Department has never compromised Ms. Attkisson's computers, or otherwise sought any information from or concerning any telephone, computer or other media device she may own or use."

51. On June 10, 2013, the independent cyber security firm hired by CBS confirmed that there was a highly sophisticated intrusion into Ms. Attkisson's computer, as well as remote actions in December, 2012, to delete all evidence of the intrusion.

52. On June 11, 2013, CBS News issued a public statement, based on the forensics report, confirming that Ms. Attkisson's computer was accessed by an unauthorized, external, unknown party on multiple occasions in late 2012, and that the party used sophisticated methods to attempt to remove all possible indications of unauthorized activity.

53. The DOJ Inspector General requested a copy of the CBS forensic expert's report and requested the opportunity to examine the Toshiba computer. CBS denied the requests. Ms. Attkisson then retained an independent computer forensics expert to conduct further analysis of the Toshiba computer.

54. In September 2013, while Ms. Attkisson continued working on the *Benghazi* story at her home in the evening, she observed for the first time that a third computer, her personal MacBook Air, was accessed remotely, controlled, and the data deleted.

55. In June of 2013, though Plaintiffs were unaware at the time, the FBI had begun conducting inquiries of Ms. Attkisson's computer intrusions under the auspices of a national security issue, but the agency failed to contact or interview Plaintiffs. Ms. Attkisson only discovered the FBI inquiry in December, 2013, when she appealed denial of her Freedom of Information Act request to the FBI and received some documents.<sup>6</sup>

56. The F.B.I. investigation involving Ms. Attkisson's computer intrusions was circulated to the DOJ's national cyber security group and included with a set of cases opened in November 2012, during the DOJ's expansion of its cyber team and the announcement of its intention to use "new tools" in its arsenal.

57. Although CBS did not release the compromised CBS computer to the DOJ Inspector General, in January 2014, Ms. Attkisson agreed to release her personal

---

<sup>6</sup> Ms. Attkisson was unaware of the F.B.I. case at the time it was opened and for months thereafter.

Apple desktop computer to the DOJ Inspector General for analysis. During the investigation, the investigators remarked to the Plaintiff that they saw a great deal of suspicious activity on the computer. However, as months went by, the DOJ Inspector General refused to release a written report to Ms. Attkisson. The DOJ Inspector General also failed to properly respond to Ms. Attkisson's subsequent Freedom of Information Act requests on the topic.

58. The DOJ Inspector General finally released a partial report upon Congressional request on the eve of Ms. Attkisson's testimony to a Senate panel in early 2015. Although the summary noted a great deal of advanced mode computer activity not attributable to Ms. Attkisson or anybody in her household, the report nonetheless concluded, paradoxically, that it found no evidence of intrusion in her personal Apple computer. The report was provided by government officials to the press. The report did not examine the compromised CBS laptop computer.

59. On January 16, 2014, and January 27, 2014, the head of the DOJ Inspector General Computer Forensics unit and a colleague visited Ms. Attkisson's home as part of the investigation, which included analysis of the Apple desktop.

60. Among other findings, Ms. Attkisson's computer forensics expert has identified an unauthorized communications channel opened into her Toshiba laptop directly connected to an Internet Provider (IP) address belonging to a federal government agency, specifically the United States Postal Service, indicating unauthorized surveillance whose source is the federal government.

61. The analysis shows the connection to a federal government agency was in use prior to January 8, 2013. The USPS has been publicly reported, including in IG internal audits,

to have a working relationship with the FBI, Department of Homeland Security, and DOJ for domestic surveillance projects.

62. Ms. Attkisson's analyst also found that while the government source who first analyzed the Toshiba laptop in January 2013, wiped evidence, there are indications that he or she likely copied and retained the evidence on an external hard drive.

63. The above-cited events, which offer only brief highlights of the cyber-attacks suffered in Plaintiffs' home, caused Plaintiffs to incur unreasonable and unnecessary expenses in an effort to diagnose and correct the problems resulting from the attacks and intrusions; resulted in an invasion of their personal and family privacy; caused them to fear for their individual and family's well-being and safety; interfered with their ability to use their telephones, computer, and television; caused them fear for her sources' well-being and safety; interfered with Plaintiffs' ability to maintain necessary contacts with sources to perform her professional investigative reporting duties as a member of the press; affected Plaintiffs' sources' willingness to communicate with her; distracted from her duties as an investigative reporter; and resulted in irreparable tension in her relationship with her employer.

64. On October 4, 2011, DOJ spokesperson Tracy Schmalter sent an email to White House Deputy Press Secretary Eric Schultz about "out of control" investigative reporter Sharyl Attkisson. This and other emails demonstrate that the Attorney General and Schmalter had become so concerned about *muzzling* Plaintiff Attkisson that Schmalter was directed to call Attkisson's editor and longtime CBS anchor Bob Scheiffer to get a "handle" on her reporting, an overt act taken to control and squash freedom of the press, her professional activities, and for political and personal reasons.

65. At the time, the White House was publicly denying any discussion about Operation *Fast and Furious* with the Attorney General or the DOJ. The Schmaler email not only proves that the DOJ and White House were jointly targeting Attkisson for political and personal reasons, but were working together to mitigate the scandal, halt Plaintiff's reporting, and to seek to use all means necessary to silence her.

66. As Plaintiff continued to report on the scandal, tensions rose at the DOJ and White House to the point that Schmaler and White House associate communications director Eric Schultz lost composure and yelled and screamed at Plaintiff Attkisson over her reporting. During this same time frame is when evidence reveals that aspects of the illegal surveillance was initiated against Plaintiffs.

67. On or about May 17, 2013, the Washington Post reported that the DOJ illegally tracked Fox News reporter James Rosen's visits to the State Department through phone traces, the timing of calls, and a review of his personal email communications in the course of a leak investigation. As was later learned, the DOJ had even illegally obtained personal phone records of Rosen's parents as part of the same course of conduct in illegally eavesdropping on the conduct of the media, including Plaintiffs.

68. During the same time period, former NSA representatives who previously left in protest of the mass privacy violations alleged to be occurring within the agency, came forward and spoke publicly confirming that agents of the United States were targeting journalists using surveillance techniques unique to the Government, further confirming that the DOJ and the agencies operating under it were targeting journalists as part of the paranoia surrounding alleged leakers using unique and state-sponsored technology.

**COUNT 1 – VIOLATION OF THE ELECTRONIC COMMUNICATIONS PRIVACY  
ACT, 18 U.S.C. §§ 2511 & 2520**

69. All prior allegations are restated herein by reference.

70. As alleged above, agents of the United States, individually and in concert, intercepted, endeavored to intercept, and/or procured another person to intercept or endeavor to intercept the Plaintiffs' wire, oral, or electronic communications.

71. Agents of the United States, individually and in concert, used, endeavored to use, and/or procured another person to use or endeavor to use and electronic, mechanical, or other device to intercept Plaintiffs' oral communications. Such device or devices were affixed to or transmitted a signal through a wire used in wire communications, and was for the purpose of obtaining information relating to business which affects interstate commerce.

72. Agents of the United States, individually and in concert, disclosed or endeavored to disclose the contents of Plaintiffs' wire, oral or electronic communications, knowing or having reason to know that the information was obtained through the interception of a wire, oral or electronic communications.

73. Upon information and belief, the above alleged conduct occurred without authorization from a court of competent jurisdiction.

74. As a direct and proximate result of the aforesaid conduct, Plaintiffs have suffered damages as set forth herein.

**COUNT 2 – VIOLATION OF THE STORED COMMUNICATIONS ACT  
18 U.S.C. §§ 2701 & 2707**

75. All prior allegations are restated herein by reference.

76. Agents of the United States, individually and in concert, intentionally accessed and/or caused to be accessed without authorization a facility through which an electronic communication service is provided, and thereby obtained Plaintiffs' wire or electronic communications while they were in electronic storage.

77. As a direct and proximate result of the aforesaid conduct, the Plaintiffs have suffered damages as set forth herein.

**COUNT 3 – VIOLATION OF THE COMPUTER FRAUD AND ABUSE ACT**  
**18 U.S.C. § 1030**

78. All prior allegations are restated herein by reference.

79. Agents of the United States, individually and in concert, intentionally accessed the Plaintiffs' computers and thereby obtained information from a protected computer, to wit Ms. Attkisson's computers used for her work as an investigative journalist for a national news agency.

80. The Defendants, individually and in concert, knowingly and intentionally accessed and/or caused to be accessed Plaintiffs' protected computers, causing interruption and interference with the ability to use such computers.

81. As a direct and proximate result of the aforesaid conduct, Plaintiffs have suffered damages as set forth herein.

**COUNT 4 – VIOLATION OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT**  
**50 U.S.C. § 1810**

82. All prior allegations are restated herein by reference.

83. The Plaintiffs were the target of electronic surveillance and/or their communications were subject to electronic surveillance at the hands or direction of agents of the United States, and therefore qualify as “aggrieved persons” per 50 U.S.C. 1801.

84. The Plaintiffs were not provided with notice of such surveillance, and upon information and belief such surveillance was not conducted pursuant to authorization from a court of competent jurisdiction.

85. As a direct and proximate result of the aforesaid conduct, the Plaintiffs have suffered damages as set forth herein.

**COUNT 5 – VIOLATION OF THE VIRGINIA COMPUTER CRIMES ACT**  
**VA. CODE § 18.2-152.12**

86. All prior allegations are restated herein by reference.

87. Agents of the United States, individually and in concert, caused the Plaintiffs’ computers to malfunction, and used or caused to be used a computer or computer network to make or cause to be made an unauthorized copy of data and communications stored in the Plaintiffs’ computers.

88. As a direct and proximate result of the aforesaid conduct, the Plaintiffs have suffered damages as set forth herein.

**COUNT 6 – COMMON LAW TRESPASS TO LAND AND CHATTEL**

89. All prior allegations are restated herein by reference.

90. Agents of the United States, individually and in concert, entered upon or caused others to enter upon the Plaintiffs’ property for purposes of installing unauthorized wire surveillance devices to conduct unlawful surveillance upon the Plaintiffs’ electronic communications.

91. Agents of the United States, individually and in concert, intruded upon or caused others to intrude upon the Plaintiffs' personal property, namely computers and other electronic devices, for purposes of conducting unlawful surveillance upon the Plaintiffs' electronic communications.

92. These trespasses to land and chattel were conducted without the Plaintiffs' consent and without lawful authority.

93. As a result of the aforesaid conduct, the Plaintiffs have suffered damages as set forth herein.

### **DAMAGES**

94. The conduct of the agents of the United States who carried out the actions described above directly and proximately caused injury to the Plaintiffs in the form of trespass upon and damage to personal property, both real and tangible, workplace harassment and intimidation, fear, stress, embarrassment, expense, inconvenience, and anxiety.

95. In an effort to discover what was happening with Ms. Attkisson's laptop and phone lines, the Plaintiffs were forced to spend a substantial amount of time and expense in investigating the maladies and hiring others to perform forensic investigations.

96. As a journalist, the ability to protect sources is crucial, and Ms. Attkisson's ability to offer such protection was compromised as a result of the surveillance giving rise to this claim.

97. This created a substantial amount of anxiety, jeopardized Plaintiff's success as a journalist, and made Plaintiff Attkisson's job more difficult than it would otherwise have been.

98. Plaintiff has incurred and will continue to incur attorneys' fees for the prosecution of this action.

### **PRAYER FOR RELIEF**

WHEREFORE, Plaintiffs request the following relief:

- A. judgment in their favor against the United States for compensatory damages in an amount to be proven at trial;
- B. for punitive damages in an amount to be proven at trial;
- C. for statutory damages pursuant to 18 U.S.C. §§ 1030, 1810, 2520 & 2707, and Virginia Code § 18.2-152.12;
- D. for their reasonable attorney's fees and costs; and
- E. for such other and further relief as the Court may deem just and appropriate.

**TRIAL BY JURY IS DEMANDED.**

RESPECTFULLY SUBMITTED,

Sharyl Thompson Attkisson  
James Howard Attkisson  
Sarah Judith Starr Attkisson

/s/ J. Gregory Webb

J. Gregory Webb, Esq. (VA Bar No. 38157)  
David W. Thomas, Esq. (VA Bar No. 73700)  
E. Kyle McNew, Esq. (VA Bar No. 73210)  
MichieHamlett PLLC  
500 Court Square, Suite 300  
Post Office Box 298  
Charlottesville, VA 22902-0298  
(434) 951-7200; (434) 951-7218 (Facsimile)  
[dthomas@michiehamlett.com](mailto:dthomas@michiehamlett.com)  
[gwebb@michiehamlett.com](mailto:gwebb@michiehamlett.com)  
[kmcnew@michiehamlett.com](mailto:kmcnew@michiehamlett.com)

and

C. Tab Turner, Esq. (*Pro Hac Vice* forthcoming)  
TURNER & ASSOCIATES, P.A.  
4705 Somers Avenue, Suite 100  
North Little Rock, Arkansas 72116  
501-791-2277 – Office  
501-791-1251 – Facsimile  
[Tab@TTurner.com](mailto:Tab@TTurner.com)